UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/007,582	12/05/2001	Roy F. Brabson	RSW920010222US1	3561

7590 01/04/2007

Jerry W. Herndon
IBM Corporation T81/503
PO Box 12195
Research Triangle Park, NC 27709

EXAMINER	
PAN, JOSEPH T	

ART UNIT	PAPER NUMBER
2135	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	01/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/007,582	BRABSON ET AL.	
	Examiner	Art Unit	
	Joseph Pan	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 September 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 December 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Applicant's response filed on September 21, 2006 has been carefully considered. Claims 1-20 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Anand et al. (U.S. Patent No. 6,370,599 B1), hereinafter referred to as Anand.

Referring to claim 1:

Anand teach:

A method of improving security processing in a computing network, comprising:

Providing a security offload component in an operating system kernel which performs security processing (see figure 2; and column 3, lines 13-60 of Anand);

Providing a control function in an operating system kernel for directing operation of the security offload component (this security offload component is

interpreted, "Figures 9 through 14 provide flowcharts which illustrate logic that may be used to implement an embodiment of the present invention which performs secure data transfer offload; and Figures 15 through 17 provide message flow diagrams showing message exchanges that may be used to implement secure handshake offload, according to another embodiment", which is in according to applicant's description on page 11, lines 13-19 of the Specification, see column 3, lines 32-36; and column 15, lines 40-56 of Anand);

Providing an application program (see abstract, lines 20-28 of Anand);

Executing the application program (see abstract, lines 20-28 of Anand); and

Executing the provided control functions. during execution of the application program, thereby directing the security offload component to secure at least one communication of the executing application program (see abstract, lines 20-28 of Anand).

Referring to claim 2:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose directing the security offload component to begin securing the communications (see column 3, lines 32-36 of Anand).

Referring to claim 3:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose directing the security offload component to stop securing the communications (see abstract, lines 26-28 of Anand).

Referring to claim 4:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose specifying information to be used by the security offload component (see column 10, lines 43-63 of Anand).

Referring to claim 5:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose the specified information including the specified encryption key, and other predefined data (see column 10, line 64 to column 11, line 12 of Anand).

Referring to claims 6-7, 16, 20:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose modifying outbound data in preparation for use by the security offload component (see column 10, lines 43-63 of Anand).

Referring to claim 8:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose the certificates (see column 2, lines 55-60; and column 10, line 64, to column 11, line 12 of Anand).

Referring to claim 9:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose the encryption key (see column 10, line 64 to column 11, line 12 of Anand).

Referring to claim 10:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose the encryption algorithm (see column 10, lines 2-4 of Anand).

Referring to claim 11:

Anand teach the claimed subject matter: a method of improving security processing in a computing network (see claim 1 above). Anand further disclose that the secured outbound data of the executing application is thereby sent to its destination directly from the security offload component, after a single path over a data bus from a protocol stack of the operating system (see figure 3; and abstract, lines 20-28 of Anand).

Referring to claim 12:

Anand teach:

A system for improving security processing in a computing network, comprising:

A security offload component in an operating system kernel which performs security processing (see figure 2; and column 3, lines 13-60 of Anand);

At least one control function in the operating system kernel for directing operation of the security offload component (see column 3, lines 32-36 of Anand);

Means for executing the at least one provided control function (see abstract, lines 20-28 of Anand); and

Means, responsive to operation of the means for executing, for directing the security offload component to secure at least one communication of an application program (see abstract, lines 20-28 of Anand).

Referring to claim 13:

Anand teach:

A computer program product for improving security processing in a computing network, the computer program product embodies on at least one computer-readable media and comprising:

A security offload component in an operating system kernel which performs security processing (see figure 2; and column 3, lines 13-60 of Anand);

At least one control function in the operating system kernel for directing operation of the security offload component (see column 3, lines 32-36 of Anand);

Computer-readable program code for executing the at least one provided control function (see column 3, lines 32-36 of Anand); and

Computer-readable program code, responsive to operation of the computer-readable program code for executing, for directing the security offload component to secure at least one communication of an application program (see abstract, lines 20-28 of Anand).

Referring to claims 14, 18:

Anand teach the claimed subject matter: a system of improving security processing in a computing network (see claim 12 above). Anand further disclose

directing the security offload component to begin securing the communications (see column 3, lines 32-36 of Anand).

Referring to claims 15, 19:

Anand teach the claimed subject matter: a system of improving security processing in a computing network (see claim 12 above). Anand further disclose directing the security offload component to stop securing the communications (see abstract, lines 26-28 of Anand).

Referring to claim 17:

Anand teach the claimed subject matter: a system of improving security processing in a computing network (see claim 12 above). Anand further disclose that the secured outbound data of the executing application is thereby sent to its destination directly from the security offload component, after a single path over a data bus from a protocol stack of the operating system (see figure 3; and abstract, lines 20-28 of Anand).

Response to Arguments

4. Applicant's arguments filed on September 21, 2006 have been fully considered but they are not persuasive.

Applicant argues:

"That is, the security offload component is provided as part of the operating system kernel software." (see page 2, second paragraph, Applicant's Arguments/Remarks)

Examiner maintains:

Applicants amended independent claims 1, 12 and 13 on October 21, 2005 to add that the security offload component is in an operating system kernel. In the Amendment, applicants state that "Support for providing the security offload component as part of the operating system kernel is provided, for example, at page 11, lines 13-19

of the Specification." (see page 1, last two lines, Applicant's Arguments/Remarks, October 21, 2005). This cited support merely discloses offload.

Applicant's specification discloses that the offload component is a hardware component in paragraphs:

"[0127] A preferred embodiment of offloading processing for security session establishment and control (and in particular, the handshake process) to an offload component will now be described with reference to the message flow diagrams in FIGS. 15 through 17. As stated earlier, this processing comprises a fourth preferred embodiment of the present invention. According to this fourth embodiment, the session establishment and control operations are processed by the **offload device** under the direction of the kernel-based SSL component. This is invoked by the Start_SSL directive being sent to the offload device. Once the Start_SSL directive is received by the offload. processing continues in one of two modes. FIGS. 15 and 16 pertain to the first mode, wherein handshake processing messages originate from the kernel. FIG. 15 depicts a first message flow for this mode, and FIG. 16 depicts a second (alternative) message flow which is preferably used when a client's Hello message arrives in a different sequence as compared to FIG. 15. FIG. 17 pertains to the second mode, wherein handshake processing begins upon receipt of a Start_SSL directive and proceeds without further interaction by the kernel, under control of the endpoints, until the handshake is complete." (see page 12, paragraph [0127], disclosing the 'offload device', of Brabson et al.)

"[0036] The present invention moves security processing (or control thereof) for security protocols such as SSL and TLS (which are connection-oriented protocols) into the kernel. In several embodiments, the security processing is performed in the TCP layer. In another embodiment, the security processing is offloaded to a component which is referred to herein as an "**encryption component**" or "**security offload component**"; in this embodiment, the TCP layer is responsible for communicating control information to the encryption component. (As will be obvious, the "encryption component" may also perform decryption.) The approach of the present invention has a

number of advantages over existing implementations that perform security functions in the application. As discussed earlier, security processing may greatly increase the complexity of application programs, and therefore moving this processing out of the application allows the programmer to focus on the task at hand; at the same time, use of the present invention enables the application to transmit and/or receive data securely. As another example, moving security processing (or control thereof) into the kernel allows layers of the stack to access clear text. This may be beneficial in many situations, such as when using kernel-based caching, which was described above." (see page 3, paragraph [0036], disclosing that an 'offload component' is referred to as an "encryption component" or "security offload component", of Brabson et al., emphasis added)

"[0048] In a sixth scenario, illustrated in FIG. 2F, SSL processing is offloaded from the stack yet remains under control of the stack. An **encryption component** such as a **hardware accelerator** (see reference number 230) may be **physically integrated** with or connected to the host in which the stack is located. In preferred embodiments, this scenario comprises reserving space for SSL protocol information (such as record number and message authentication code) in data packets which are processed by the IP layer, and passing control information (such as lengths and offset values to be used when encrypting data, digital certificates of the client and server, keys or file names of key rings to be used per connection, the encryption algorithm to be used, etc.) between the offloading stack and the encryption component. In addition, directives such as "Start_SSL" and "Stop_SSL" may be communicated from the offloading stack to the encryption component to direct it when to start or stop performing security functions on the data it receives. Arrow 240 generally represents the exchange of directives and data between the stack and the encryption component. Offloading of decryption may be performed in a similar manner. This offloading technique may be used with any of the application scenarios previously described (including those that issue SSL directives from an application and those that issue SSL calls which operate as no-ops), for applications that are SSL-enabled, SSL-aware, or neither SSL-enabled nor SSL-aware." (see page 5, paragraph [0048], disclosing that "an encryption component" [i.e., "an

offload component"] such as a hardware accelerator may be physically integrated with or connected to the host", of Brabson et al., emphasis added)

"[0091] A preferred embodiment of the offload processing for data transfer, which corresponds to the sixth scenario discussed above, will now be described with reference to FIGS. 9 through 14. As was stated, this processing comprises a third preferred embodiment of the present invention. FIG. 9 depicts outbound processing occurring in the stack of a server, and FIG. 10 depicts outbound processing for the offload component (which is also referred to as "the adapter"). FIG. 11 is described next, and shows how inbound processing may be performed for a client. FIG. 12 then provides outbound client processing. FIG. 13 provides inbound offload processing, and finally, FIG. 14 provides inbound processing at the server." (see page 9, paragraph [0091], disclosing the "offload component" is also referred as "the adapter", of Brabson et al., emphasis added). What Anand anticipates is providing a security offload component in an operating system kernel which performs security processing.

Applicant argues:

"...Anand inherently does not disclose or suggest the recitation "providing control functions in the operating system kernel for directing operation of the security offload component" (see page 3, 1st paragraph, Applicant's Arguments/Remarks)

Examiner maintains:

Anand discloses that "In a computer system environment having an operating system and at least one peripheral hardware device, a method for dynamically offloading, on a per-packet basis and depending on the then current needs of the computer system, an operating task from the operating system to the peripheral hardware device, thereby freeing up host processor resources and increasing the overall efficiency of the computer system, the method comprising:

a step for ascertaining, by the operating system, task offload capabilities of the peripheral hardware device;

a step for enabling, by the operating system, selected task offload capabilities of the peripheral hardware device that are selected from among the ascertained task

offload capabilities, said selected task offload capabilities being enabled to the extent such selected task offload capabilities are needed for one or more data packets;" (see column 15, lines 40-56 of Anand, emphasis added).

Thus, Anand discloses providing control functions in the operating system kernel for directing operation of the security offload component.

Conclusion

5. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph Pan whose telephone number is 571-272-5987.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100